



**Thinstuff Touch RDP Server**  
Small Business Edition 1.0

**User Manual**

## Table of Contents

1	Installation .....	3
1.1	Introduction .....	3
1.2	Installation steps .....	3
1.3	Installed files.....	3
2	Operation .....	4
2.1	Configuration via webserver .....	4
2.2	Cluster Status.....	4
2.2.1	Cluster Health.....	4
2.2.2	License Info.....	5
2.3	Sessions.....	6
2.4	Rights.....	6
2.4.1	Users .....	6
2.4.2	Groups .....	8
2.5	Settings .....	8
2.5.1	Profiles.....	8
2.5.2	Global Settings.....	9
2.5.3	Profile Settings.....	9
2.5.4	Default Settings .....	10
2.6	Advanced configuration.....	10
2.6.1	Database configuration.....	10
2.6.2	Web server configuration.....	11
3	How-to .....	12
3.1	Profile Questions.....	12
4	Limitations.....	13
5	Compatibility.....	13
5.1	RDP Clients .....	13
5.2	Hardware and Software.....	13
	Appendix A – Settings Descriptions.....	15

## 1 Installation

### 1.1 Introduction

This manual assumes basic familiarity with the Linux™ operating system and your current desktop environment (e.g.: Gnome or KDE). Furthermore you will need to be a privileged user (ie: root user) to install the package successfully, installation as a normal user is not currently supported. If you do not have the possibility to install the package as a privileged user yourself, please ask your system administrator for assistance.

### 1.2 Installation steps

As a privileged user, open a console at the location where you downloaded the installation package.

Execute the installation script by typing:

```
sh ./rdpserver-sbs-1.0.sh
```

Follow the instruction on the screen to install the RDP server.

If you do not already have a license, obtain a trial license from  
<http://www.thinstuff.com/licensing>

Place that license into the folder `/opt/thinstuff/rdpserver/licenses`

### 1.3 Installed files

All files are installed in the directory `/opt/thinstuff/rdpserver`. To uninstall the package it is sufficient to delete this directory. The package needs about 132 megabytes of disk space for installation and operation. The following files are of particular interest:

- `/opt/thinstuff/rdpserver/scripts/startall.sh`  
Start the small business server.
- `/opt/thinstuff/rdpserver/scripts/stopall.sh`  
Stop the small business server.
- `/opt/thinstuff/rdpserver/scripts/init.sh`  
Restart the small business server, this has the same effect as calling `stopall.sh` followed by `startall.sh`

## 2 Operation

### 2.1 Configuration via webserver

The small business server is administered via a web based configuration and management interface. After installing and starting your server, please point your web browser to <https://my.server.url/> (Please see section 2.6.2 if you need to start the web service on a different port, also note that the default setting is the https protocol instead of simple http).

Please log in as user "root" with your current root password (see section 2.4 on how to configure access for different users). The web interface is split into 4 areas:

- **Cluster Status** – Determine current problems quickly
- **Sessions** – Identify which user is using your services and manage them
- **Rights** – Configure who has access to the web interface
- **Settings** – Configure operational parameters for the terminal server and sessions

### 2.2 Cluster Status

#### 2.2.1 Cluster Health

In this section you can get a quick overview of the status of your terminal server. The status is color-coded for easy reference, and eventual problems will show explanatory status messages. There are four different status levels:

Cluster and Server Status	
The following information provides an overview about the cluster and server status managed through the Thinstuff Touch Terminal Server.	
Element	Status
Small Business Server Status	RUNNING
License Status	Grace
Number of currently active sessions	0
Number of currently active connections	0
Status messages:	<ul style="list-style-type: none"> <li>• no messages</li> </ul>

- **Running (green)** – Everything is working without problems
- **Warning (yellow)** – The server is working, but one or more components are experiencing problems. It is advised to monitor server behavior to see if the problem is just temporary or to upgrade overloaded resources. Problems could include:

- CPU, Memory or other resources reach a critical point
- One or more, but not all, copies of a redundant component are reporting errors during operation.
- **Critical (red)** – Similar problems like Warning, but they affect all copies of a redundant component or a non-redundant component. If a server is in status critical then it may still work, but it might fail soon or not work reliable for all connections. It is advised to restart the terminal server as soon as this is conveniently possible, and to upgrade overloaded resources or increase redundancy.
- **Error (red)** – One or more components have definitely failed and the server is not operational anymore. You will need to restart the terminal server.

### 2.2.2 License Info

The second part of the Cluster Status section shows you information about your current licenses. The top part shows a summary, and it will display the effective license values. If some of these values are based on licenses in grace mode (see below) then this section will be marked yellow, otherwise it is marked green.

Cluster Status	Sessions	Rights	Settings			
Cluster Health	License Info					
<b>License Information</b>						
<b>Effective/Combined license information</b>						
<b>Combined license data</b>						
License state:						
Max number of configuration servers:						
Max number of application launchers:						
Max number of proxy servers:						
Max number of Xoops:						
Max number of concurrent connections:						

Below this section you will see information about every license file found in your licenses folder (`/opt/thinstuff/rdpserver/licenses`). Each license can be in one of three states:

- **Valid (green)** – The license is still fully valid
- **Grace (yellow)** – The license is already expired, but is valid a little longer (see the information about when the grace period expires). If a connection to the terminal server is accepted only because of a license in grace period, then the user will be notified of this by a message prior to connecting. Also licenses may have additional restrictions (fewer connections, ...) during the grace period.
- **Invalid (red)** – This may have various reasons (invalid hardware id, invalid license file, ...).

A valid license will show values for normal operation and grace operation. The color coding will show which values are in effect currently and when the license will cease to be valid.

License state:	License number:	54
Filename:	Valid	
<b>License state:</b>		
<b>Grace</b>		
Filename:	/opt/thinstuff/rdpserver/licenses/lc2.lc	
Expiration:	2006-01-01	
Max number of configuration servers:	0	
Max number of application launchers:	0	
Max number of proxy servers:	0	
Max number of Xoops:	0	
Max number of concurrent connections:	1	
Expiration (in grace mode):	2007-01-01	
Max number of configuration servers (in grace mode):	0	
Max number of application launchers (in grace mode):	0	
Max number of proxy servers (in grace mode):	0	
Max number of Xoops (in grace mode):	0	
Max number of concurrent connections (in grace mode):	1	

## 2.3 Sessions

This section will list all currently active sessions and connections for the terminal server. Each sessions can have zero, one or more connections. Sessions with zero connections do not currently have users viewing them and will be automatically destroyed after the given session timeout. Sessions with more than one connection are shadowed by one or more users.

Sessions									
ID	Node ID	User ID	Initial Client Host	Profile ID	Pid	Clients Connected	Last Disconnect Time	Session Timeout	Actions
33	-1	se2031	CADR3MA	default	29244	1		-1	<a href="#">Filter Connections</a> <a href="#">Destroy Session</a>
34	-1	autoUser	CADR3MA	tom	29293	1		0	<a href="#">Filter Connections</a> <a href="#">Destroy Session</a>

  

All Connections									
ID	Proxy	Client IP	Client Port	Session ID	Username	Resolution	Locale	Actions	
18	30	192.168.0.21	1253	33	se2031	800x600x24	en_US	<a href="#">Disconnect</a>	
19	30	192.168.0.21	1255	34	not available	800x600x24	en_US	<a href="#">Disconnect</a>	

It is possible to destroy a complete session (all connected users will be disconnected) or just a single connection (the session is unaffected, but the timeout may eventually destroy the session if the last connection is removed).

To quickly see which connections are viewing a given session, press the “Filter Connections” button. Only this session, and only connections for this session will be shown until the “Show all” button is pressed.

Thinstuff Touch Terminal Server									
Sessions									
ID	Node ID	User ID	Initial Client Host	Profile ID	Pid	Clients Connected	Last Disconnect Time	Session Timeout	Actions
33	-1	se2031	CADR3MA	default	29244	1		-1	<a href="#">Filter Connections</a> <a href="#">Destroy Session</a>

  

Connections for Session 33									
ID	Proxy	Client IP	Client Port	Session ID	Username	Resolution	Locale	Actions	
18	30	192.168.0.21	1253	33	se2031	800x600x24	en_US	<a href="#">Disconnect</a>	

## 2.4 Rights

The website and the terminal server use system users and passwords for authentication. Not every user has access to the web interface though. The access to the web interface and the rights to view/modify different settings can be configured per user. After the installation the root user has full access (all rights) and no other user has any rights.

### 2.4.1 Users

This section shows all the known users in the system. This list is synchronized with the system every few seconds, so if you add new system users they should show up here a few seconds later. For every user the list of groups this user is member in is also shown. Click a group to see the groups list with this group highlighted.

Thinstuff Touch Terminal Server									
Users									
ID	Name	UID	Groups			Home Directory	Shell	Actions	
4	adm	3	sys adm disk			/var/adm	/bin/false	<a href="#">Rights</a>	
31	alias	200	nologin			/var/empty/alias	/bin/false	<a href="#">Rights</a>	
16	apache	81	apache			/var/www	/bin/false	<a href="#">Rights</a>	
18	at	25	at			/var/spool/cron/atjobs	/bin/false	<a href="#">Rights</a>	
43	authuser	1003	users			/home/authuser	/bin/bash	<a href="#">Rights</a>	
2	bin	1	bin daemon sys			/bin	/bin/false	<a href="#">Rights</a>	
15	cron	16	cron			/var/spool/cron	/bin/false	<a href="#">Rights</a>	
28	cyrus	85	mail			/var/cyrus	/bin/false	<a href="#">Rights</a>	
3	daemon	2	bin daemon adm			/bin	/bin/false	<a href="#">Rights</a>	
16	ftp	21	ftp			/home/ftp	/bin/false	<a href="#">Rights</a>	
22	games	35	games users			/var/games	/bin/false	<a href="#">Rights</a>	
20	gdm	32	gdm			/var/lib/gdm	/bin/false	<a href="#">Rights</a>	
8	halt	7	root			/bin	/sbin/halt	<a href="#">Rights</a>	
41	ldap	439	ldap			/usr/lib/ldap	/bin/false	<a href="#">Rights</a>	
5	lp	4	lp			/var/spool/lpd	/bin/false	<a href="#">Rights</a>	
9	mail	8	mail			/var/spool/mail	/bin/false	<a href="#">Rights</a>	
13	man	13	man			/usr/share/man	/bin/false	<a href="#">Rights</a>	
24	mysql	60	mysql			/var/lib/mysql	/bin/false	<a href="#">Rights</a>	

Click on the Rights link to view the rights assigned to this user.

In this view you can see which rights are set for the groups the user is member of, for the user itself, and what effective rights this results in. Right composition follows the following rules (in this order):

1. User rights override group rights. If a right is set for a user this is used, otherwise the group rights are used.
2. Group rights are merged. It is sufficient to have "Allow"/"Deny" set in one of the groups a user is member of.
3. "Deny" overrides "Allow":
  - a. If a user has "Allow" set, but inherits "Deny" from group rights, then the final right is "Deny".
  - b. If the groups a user is member of have both "Allow" and "Deny" set then the group right is "Deny".
4. If rules 1 to 3 do not produce any result (nothing set) then the resulting right is "Deny".

Thinstuff Touch Terminal Server																											
Cluster Status		Sessions		Rights		Settings																					
Users		Groups																									
<b>Composed rights for user adm</b>																											
<a href="#">Switch to full mode</a>																											
<b>Group Rights</b>																											
Rights of the selected group or of all groups assigned to the selected user.																											
Groupname(GID)		Login		Rights		Users		Groups		Profiles		Settings		Nodes													
sgp(3)		View		Change		View		Change		View		Change		View													
adm(4)		View		Change		View		Change		View		Change		View													
grp(4)		View		Change		View		Change		View		Change		View													
<a href="#">Edit Rights</a>																											
<b>User Rights</b>																											
Rights of the selected user or of all users assigned to the selected group.																											
Username(UID)		Login		Rights		Users		Groups		Profiles		Settings		Nodes													
adm(3)		View		Change		View		Change		View		Change		View													
<a href="#">Edit Rights</a>																											
<b>Composed Rights</b>																											
Effective rights for the selected user. The rights are effectively in use and consist of all group and user rights of the selected user.																											
Username(UID)		Login		Rights		Users		Groups		Profiles		Settings		Nodes													
adm(3)		D		D		D		D		D		D		D													

There are currently 19 rights:

- **Login** – This user is allowed to log on to the web interface. This is a prerequisite for all of the other rights.
- **View/Change Rights** – View or change the assignment of rights. With this and all the other rights which have a "View" and "Change" representation the "View" version gives read-only access, while the "Change" version allows modification. Typically "View" is a prerequisite for "Change" since the user interface needs to display the values before you can change them.
- **View/Change Users** – View or change the list of system users.
- **View/Change Groups** – View or change the list of system groups.
- **View/Change Profiles** – View or change the profiles (see section ??) the terminal server uses.
- **View/Change Settings** – View or change the settings (see section ??) the terminal server uses.
- **View/Change Nodes** – This is only for clustered servers, it is not currently in use

- **View/Change Services** – This is only for clustered servers, it is not currently in use
- **View/Change Sessions** – View or change (destroy) sessions (see section 2.3)
- **View/Change Connections** – View or change (destroy) connections (see section 2.3)

Note, that some of these rights are prerequisites for other rights. For example it is necessary to have at least read-only access to the user list to be able to view or change user rights.

## 2.4.2 Groups

Same as the user list, this shows all the known groups in the system. This list is also synchronized with the system every few seconds. Click on a member of a group to show the user list with this member highlighted. Click the rights link to change the rights for this group (analogous to the user rights dialog).

Groups			Users	Actions
ID	Name	GID		
5	adm	4	root daemon adm	Rights
35	apache	81	apache	Rights
24	at	25	at	Rights
19	audio	18		Rights
2	bin	1	root bin daemon	Rights
20	cdrom	19		Rights
34	cdrw	80		Rights
18	console	17		Rights
17	cron	16	cron	Rights
3	daemon	2	root bin daemon	Rights
21	dialout	20	root	Rights
7	disk	6	root adm	Rights

## 2.5 Settings

Settings govern different aspects of the terminal server behavior. These range from port allocation to various CPU or bandwidth optimizations. There are two different kinds of settings:

- **Global Settings** – They are always valid, and are independent of individual sessions or connections. They include things like the port the RDP server listens for connections.
- **Profile Settings** – These are only valid for a given session or connection. Each session and connection run under a specific profile, and different profiles can have different values for those settings.

## 2.5.1 Profiles

It is often necessary to change settings based on which user is connecting to the server, where this user is coming from or which hardware this user has. To allow this, the terminal server has the concept of profiles. Each profile stores a set of setting values, and whenever a client connects to the server, a profile is selected based on one or more of the following criteria:

- Username
- Groupname
- Hostname

When multiple profiles would match the current connection, then the most specific match is chosen. Should there be a tie in the match, then the following order of priority is used:

1. Matching username
2. Matching default group of this user
3. Matching group of this user
4. Matching hostname

Once the profile is selected the settings in this profile apply for that client. Which of these values applies is governed through the “Match” group of profile settings (see below). Profiles can also be “passive” (deactivated). In this mode they will never match any user.

There exist two exceptions to this rule:

- During login, a user will always be in the special “login” profile.
- If a user connects to an already existing session (by reconnect or by shadowing) then he will use the profile the session had when it was first created.

### 2.5.2 Global Settings

Global settings are settings which are needed during server startup or at other times when a matching into profiles is not possible. To get explanation of the settings, move your mouse over the setting name, and a popup window will show you help information. Additionally the information will be displayed when you edit a value.

Thinstuff Touch Terminal Server			
Cluster Status		Sessions	Rights
Global Settings		Profiles	Default Settings
<b>Settings</b>			
<b>Global Settings</b>			
These settings are the effective global settings. The <span style="background-color: #008000; color: white;">green</span> settings are different from the default value.			
<a href="#">Change view to overridden global settings</a>			
<b>ID</b>	<b>Name</b>	<b>Value</b>	<b>Actions</b>
602	Security.RDP.ProtocolVersion	5	<a href="#">Edit value</a>
603	Security.RDP.CryptoVersion	5	<a href="#">Edit value</a>
604	Security.RDP.KeyLength	16	<a href="#">Edit value</a>
605	Security.RDP.ServerCert	/opt/thinstuff/rdpserver/keys/servercert.pem	<a href="#">Edit value</a>
606	Security.RDP.ClientCert	/opt/thinstuff/rdpserver/keys/clientcert.pem	<a href="#">Edit value</a>
607	Security.RDP.ServerKey	/opt/thinstuff/rdpserver/keys/serverkey.pem	<a href="#">Edit value</a>
608	Security.RDP.CACert	/opt/thinstuff/rdpserver/keys/cacert.pem	<a href="#">Edit value</a>
610	Security.Authentication.performEarlyAuthentication	true	<a href="#">Edit value</a>
611	Security.Authentication.overrideSessionTimeout	true	<a href="#">Edit value</a>

### 2.5.3 Profile Settings

In this section you can change profile settings as well as manage the profiles themselves. Click on “Edit value” for a specific setting to change it. The help text will be displayed also in the edit dialog, for easy reference.

Settings			
Profile Selection			
Selected Profile: 2.default <a href="#">Change profile</a>			
Passive profile: <input checked="" type="checkbox"/> <a href="#">Deactivate Profile</a>			
Deleting the selected profile			
Do you want to delete the profile? <a href="#">Delete profile</a>			
Creating a new profile			
New profile name: <input type="text"/> <a href="#">Create profile</a>			
Passive profile: <input type="checkbox"/>			
Copy from selected: <input type="checkbox"/>			
<b>Settings</b>			
These settings are the effective settings for the selected profile. The <span style="background-color: #008000; color: white;">green</span> settings are different from the default value.			
<a href="#">Change view to overridden profile specific settings</a>			
<b>ID</b>	<b>Name</b>	<b>Value</b>	<b>Actions</b>
101	ApplicationLauncher.xservercheck.sleep	500	<a href="#">Edit value</a>
102	ApplicationLauncher.xservercheck.retries	20	<a href="#">Edit value</a>
103	ApplicationLauncher.xservercheck.lorTimeout	5	<a href="#">Edit value</a>
104	ApplicationLauncher.Authentication.authClientTimeout	160	<a href="#">Edit value</a>
105	ApplicationLauncher.Authentication.authClientTimeout2	20	<a href="#">Edit value</a>
201	Session.timeout	-1	<a href="#">Edit value</a>
202	Session.timeout	The timeout in seconds, until a running session without connected clients is kept. If the value is set to -1 it means forever, 0 means that the session is killed after the last client disconnects.	<a href="#">Edit value</a>
203	Session.timeout	The timeout in seconds, until a running session without connected clients is kept. If the value is set to -1 it means forever, 0 means that the session is killed after the last client disconnects.	<a href="#">Edit value</a>
204	Session.timeout	The timeout in seconds, until a running session without connected clients is kept. If the value is set to -1 it means forever, 0 means that the session is killed after the last client disconnects.	<a href="#">Edit value</a>

## 2.5.4 Default Settings

In this section you can view and change the system defaults for settings. It is not recommended that you actually change system defaults since there is no convenient way to reset them back to factory defaults.

## 2.6 Advanced configuration

Some configurations are not possible via the web interface. These include the configuration of basic services, like the webserver or the database server which are needed by the web interface to work properly.

Thinstuff Touch Terminal Server																																																																											
Cluster Status	Sessions	Rights	Settings																																																																								
<a href="#">Global Settings</a> <a href="#">Profiles</a> <a href="#">Default Settings</a>																																																																											
<b>Settings</b>																																																																											
<b>Default Settings</b>																																																																											
<table border="1"> <thead> <tr> <th>ID</th> <th>Name</th> <th>Value</th> <th>Action</th> </tr> </thead> <tbody> <tr><td>602</td><td>Security.RDP.ProtocolVersion</td><td>5</td><td><a href="#">Edit Value</a></td></tr> <tr><td>603</td><td>Security.RDP.CryptoVersion</td><td>5</td><td><a href="#">Edit Value</a></td></tr> <tr><td>604</td><td>Security.RDP.KeyLength</td><td>16</td><td><a href="#">Edit Value</a></td></tr> <tr><td>605</td><td>Security.RDP.ServerCert</td><td>/opt/thinstuff/rdpserver/keys/servercert.pem</td><td><a href="#">Edit Value</a></td></tr> <tr><td>606</td><td>Security.RDP.ClientCert</td><td>/opt/thinstuff/rdpserver/keys/clientcert.pem</td><td><a href="#">Edit Value</a></td></tr> <tr><td>607</td><td>Security.RDP.ServerKey</td><td>/opt/thinstuff/rdpserver/keys/serverkey.pem</td><td><a href="#">Edit Value</a></td></tr> <tr><td>608</td><td>Security.RDP.CACert</td><td>/opt/thinstuff/rdpserver/keys/cacert.pem</td><td><a href="#">Edit Value</a></td></tr> <tr><td>610</td><td>Security.Authentication.performEarlyAuthentication</td><td>true</td><td><a href="#">Edit Value</a></td></tr> <tr><td>611</td><td>Security.Authentication.performRateAuthentication</td><td>true</td><td><a href="#">Edit Value</a></td></tr> <tr><td>612</td><td>Security.Authentication.authenticationUsername</td><td>authuser</td><td><a href="#">Edit Value</a></td></tr> <tr><td>613</td><td>Security.Authentication.authenticationProfile</td><td>login</td><td><a href="#">Edit Value</a></td></tr> <tr><td>614</td><td>Security.Authentication.alwaysShowChooser</td><td>false</td><td><a href="#">Edit Value</a></td></tr> <tr><td>901</td><td>Network.RDP.port</td><td>3389</td><td><a href="#">Edit Value</a></td></tr> <tr><td>902</td><td>Network.ConnectionForwarding.timeout.sec</td><td>0</td><td><a href="#">Edit Value</a></td></tr> <tr><td>903</td><td>Network.ConnectionForwarding.timeout.usec</td><td>250000</td><td><a href="#">Edit Value</a></td></tr> <tr><td>904</td><td>Network.ConnectionForwarding.socketRange.mn</td><td>100001</td><td><a href="#">Edit Value</a></td></tr> <tr><td>905</td><td>Network.ConnectionForwarding.socketRange.max</td><td>10501</td><td><a href="#">Edit Value</a></td></tr> </tbody> </table>				ID	Name	Value	Action	602	Security.RDP.ProtocolVersion	5	<a href="#">Edit Value</a>	603	Security.RDP.CryptoVersion	5	<a href="#">Edit Value</a>	604	Security.RDP.KeyLength	16	<a href="#">Edit Value</a>	605	Security.RDP.ServerCert	/opt/thinstuff/rdpserver/keys/servercert.pem	<a href="#">Edit Value</a>	606	Security.RDP.ClientCert	/opt/thinstuff/rdpserver/keys/clientcert.pem	<a href="#">Edit Value</a>	607	Security.RDP.ServerKey	/opt/thinstuff/rdpserver/keys/serverkey.pem	<a href="#">Edit Value</a>	608	Security.RDP.CACert	/opt/thinstuff/rdpserver/keys/cacert.pem	<a href="#">Edit Value</a>	610	Security.Authentication.performEarlyAuthentication	true	<a href="#">Edit Value</a>	611	Security.Authentication.performRateAuthentication	true	<a href="#">Edit Value</a>	612	Security.Authentication.authenticationUsername	authuser	<a href="#">Edit Value</a>	613	Security.Authentication.authenticationProfile	login	<a href="#">Edit Value</a>	614	Security.Authentication.alwaysShowChooser	false	<a href="#">Edit Value</a>	901	Network.RDP.port	3389	<a href="#">Edit Value</a>	902	Network.ConnectionForwarding.timeout.sec	0	<a href="#">Edit Value</a>	903	Network.ConnectionForwarding.timeout.usec	250000	<a href="#">Edit Value</a>	904	Network.ConnectionForwarding.socketRange.mn	100001	<a href="#">Edit Value</a>	905	Network.ConnectionForwarding.socketRange.max	10501	<a href="#">Edit Value</a>
ID	Name	Value	Action																																																																								
602	Security.RDP.ProtocolVersion	5	<a href="#">Edit Value</a>																																																																								
603	Security.RDP.CryptoVersion	5	<a href="#">Edit Value</a>																																																																								
604	Security.RDP.KeyLength	16	<a href="#">Edit Value</a>																																																																								
605	Security.RDP.ServerCert	/opt/thinstuff/rdpserver/keys/servercert.pem	<a href="#">Edit Value</a>																																																																								
606	Security.RDP.ClientCert	/opt/thinstuff/rdpserver/keys/clientcert.pem	<a href="#">Edit Value</a>																																																																								
607	Security.RDP.ServerKey	/opt/thinstuff/rdpserver/keys/serverkey.pem	<a href="#">Edit Value</a>																																																																								
608	Security.RDP.CACert	/opt/thinstuff/rdpserver/keys/cacert.pem	<a href="#">Edit Value</a>																																																																								
610	Security.Authentication.performEarlyAuthentication	true	<a href="#">Edit Value</a>																																																																								
611	Security.Authentication.performRateAuthentication	true	<a href="#">Edit Value</a>																																																																								
612	Security.Authentication.authenticationUsername	authuser	<a href="#">Edit Value</a>																																																																								
613	Security.Authentication.authenticationProfile	login	<a href="#">Edit Value</a>																																																																								
614	Security.Authentication.alwaysShowChooser	false	<a href="#">Edit Value</a>																																																																								
901	Network.RDP.port	3389	<a href="#">Edit Value</a>																																																																								
902	Network.ConnectionForwarding.timeout.sec	0	<a href="#">Edit Value</a>																																																																								
903	Network.ConnectionForwarding.timeout.usec	250000	<a href="#">Edit Value</a>																																																																								
904	Network.ConnectionForwarding.socketRange.mn	100001	<a href="#">Edit Value</a>																																																																								
905	Network.ConnectionForwarding.socketRange.max	10501	<a href="#">Edit Value</a>																																																																								
<b>Profile Specific Default Settings</b>																																																																											
<table border="1"> <thead> <tr> <th>ID</th> <th>Name</th> <th>Value</th> <th>Action</th> </tr> </thead> <tbody> <tr><td>101</td><td>ApplicationLauncher.xsavercheck.sleep</td><td>500</td><td><a href="#">Edit Value</a></td></tr> <tr><td>102</td><td>ApplicationLauncher.xsavercheck.retries</td><td>20</td><td><a href="#">Edit Value</a></td></tr> <tr><td>103</td><td>ApplicationLauncher.xsavercheck.orTimeout</td><td>5</td><td><a href="#">Edit Value</a></td></tr> <tr><td>104</td><td>ApplicationLauncher.Authentication.authclientTimeout</td><td>160</td><td><a href="#">Edit Value</a></td></tr> <tr><td>105</td><td>ApplicationLauncher.Authentication.authclientTimeout2</td><td>20</td><td><a href="#">Edit Value</a></td></tr> <tr><td>201</td><td>Session.timeout</td><td>-1</td><td><a href="#">Edit Value</a></td></tr> <tr><td>202</td><td>Session.startApplication</td><td>true</td><td><a href="#">Edit Value</a></td></tr> <tr><td colspan="4"><small>© 2006 Thinstuff s.r.o. All rights reserved. Thinstuff is a registered trademark of Thinstuff s.r.o.</small></td></tr> </tbody> </table>				ID	Name	Value	Action	101	ApplicationLauncher.xsavercheck.sleep	500	<a href="#">Edit Value</a>	102	ApplicationLauncher.xsavercheck.retries	20	<a href="#">Edit Value</a>	103	ApplicationLauncher.xsavercheck.orTimeout	5	<a href="#">Edit Value</a>	104	ApplicationLauncher.Authentication.authclientTimeout	160	<a href="#">Edit Value</a>	105	ApplicationLauncher.Authentication.authclientTimeout2	20	<a href="#">Edit Value</a>	201	Session.timeout	-1	<a href="#">Edit Value</a>	202	Session.startApplication	true	<a href="#">Edit Value</a>	<small>© 2006 Thinstuff s.r.o. All rights reserved. Thinstuff is a registered trademark of Thinstuff s.r.o.</small>																																							
ID	Name	Value	Action																																																																								
101	ApplicationLauncher.xsavercheck.sleep	500	<a href="#">Edit Value</a>																																																																								
102	ApplicationLauncher.xsavercheck.retries	20	<a href="#">Edit Value</a>																																																																								
103	ApplicationLauncher.xsavercheck.orTimeout	5	<a href="#">Edit Value</a>																																																																								
104	ApplicationLauncher.Authentication.authclientTimeout	160	<a href="#">Edit Value</a>																																																																								
105	ApplicationLauncher.Authentication.authclientTimeout2	20	<a href="#">Edit Value</a>																																																																								
201	Session.timeout	-1	<a href="#">Edit Value</a>																																																																								
202	Session.startApplication	true	<a href="#">Edit Value</a>																																																																								
<small>© 2006 Thinstuff s.r.o. All rights reserved. Thinstuff is a registered trademark of Thinstuff s.r.o.</small>																																																																											

### 2.6.1 Database configuration

The default database configuration accepts incoming connections on TCP port 15432 and is bound to localhost. The default UNIX sockets for the postgres database are stored in /opt/thinstuff/rdpserver/var/lib/postgres.

The default user for the integrated postgres daemon is thinstuffpostgres. This should prevent any naming and user conflicts with existing postgres installations.

The following problems arise with the default setup:

- any user with access to the postgres TCP socket from the local machine can open a connection to the database
- the default port may already be used by other services on the target server

#### 2.6.1.1 Securing Postgres

Postgres can be secured by setting a password for the user and only allowing connections from the respective Thinstuff Touch configuration server.

Please execute the following steps (the script psql-wrapper.sh is provided to make sure the bundled postgres client is used):

1. Open the postgres command line client (type the command in your shell):

```
cd /opt/thinstuff/rdpserver/scripts
./psql-wrapper.sh -U thinstuffpostgres \
-h /opt/thinstuff/rdpserver/var/lib/postgres \
-p 15432 terminalserver
```

2. Within psql type (replace new-password with your new server password):

```
ALTER ROLE thinstuffpostgres WITH PASSWORD 'new-password';
```

3. Update pg\_hba.conf to disable the TCP sockets

pg\_hba.conf has a lot of documentation inside on how to configure access to the postgres database. For a typical localhost only installation the only active line should be:

local	terminalserver	thinstuffpostgres	password
-------	----------------	-------------------	----------

4. Update the configuration server config files

Open the INI-configuration file configurationserver.ini at /opt/thinstuff/rdpserver/etc/thinstuff.

At the beginning of the file you will find the section [Database]. Within the section you can find the Pass= entry which is empty by default. Please update it with the database you have used for the thinstuffpostgres user.

### **2.6.1.2 Changing the Database Port**

The database port can be changed in postgresql.conf located in the directory /opt/thinstuff/rdpserver/var/lib/postgres/data.

There you will find the setting port which is 15432 by default. Change it to a free port on your system.

After changing the database port the configurationserver.ini configuration file at /opt/thinstuff/rdpserver/etc/thinstuff has to be updated to use the new port.

At the beginning of the file you will find the section [Database], please change the setting Port to the new database port.

### **2.6.2 Web server configuration**

The terminal server uses lighttpd (<http://www.lighttpd.net/>) as web-server component lighttpd

It can be configured with the included and documented lighttpd configuration file which can be found at:

/opt/thinstuff/rdpserver/etc/lighttpd/lighttpd.conf.
--

If you need to change the port the web server listens on, change to value "server.port" to your desired port (default is 443 for https operation). If you want to disable https, then please change "ssl.engine" to "disable". Note that in that case you also should change the web port to 80, this does not happen automatically.

For more information about lighttpd configuration, please see <http://trac.lighttpd.net/trac/wiki>

Reference of the most important settings:

- **server.port** – change the port of the web server (default: 443/https), this is especially necessary if another web server using port 443 is running on the same host as the terminal server
- **server.bind** – change the address the web server is bound to (default: any interface)
- **ssl.engine** – enable or disable the SSL mode (default: enable)
- **ssl.pemfile** – the PEM file which contains the server SSL private key and client certificate (change this to your SSL certificate to use it instead of the default self-signed certificate)

## 3 How-to

### 3.1 Profile Questions

**?** How do I change which window manager or desktop environment a specific profile uses?

1. Go to Settings -> Profiles
2. Select the profile you want to modify
3. change "Applications.session.command" to the command to execute your desired window manager. Some choices include:
  - a. /opt/thinstuff/rdpserver/bin/twm – Use the included twm window manager (default value)
  - b. startkde – Start a KDE session.
  - c. gnome-session – Start a Gnome session.
  - d. icewm-session – Start the Icewm window manager.

**?** How do I create a profile with specific values for a certain user/group/hostname?

1. Go to Settings -> Profiles
2. Select the profile you want to base your new profile on

3. Enter a new profile name
4. Check “Copy from selected” if you want to copy the values from the selected profile. Otherwise every value will be set to the default values.
5. Change the value for “Match.users.enable” to true to enable matching specific user names (analogous use “Match.groups.enable” or “Match.hosts.enable” for groups or hostnames)
6. Edit the value “Match.users.values” and add the usernames you want to match.
7. Edit profile the other profile settings to the desired values.
8. Test it. You should now get the specified profile settings when connecting with the given user.

## 4 Limitations

The small business edition is limited in the following aspects:

- All components must run on the same server.
- Configuration must be done via the web interface. File based configuration is not possible.

## 5 Compatibility

### 5.1 RDP Clients

The server is tested to be compatible with the following RDP Clients:

- rdesktop 1.3.1
- rdesktop 1.4
- Microsoft RDP Client 5.1.2600.0 (Windows XP)
- Microsoft RDP Client 5.1.2600.1160 (Windows XP, SP1)
- Microsoft RDP Client 5.2.3790 (Windows XP, SP2)

The following clients work, but because of certain incompatibilities might run slower than expected:

- Microsoft RDP Client 5.0 (Windows 2000)
- Microsoft RDP Client on Windows CE 5.0

### 5.2 Hardware and Software

The package will run on all 32-bit x86 Linux based distributions with 32-bit glibc 2.2.5 or higher, a 32-bit PAM library (pam.so) and kernel versions 2.4.x or 2.6.x.

On 64-bit Linux systems which support 32-bit applications (Opteron, Athlon 64, ...) it might be required to install compatibility libraries.

## Thinstuff Touch RDP Server – User Manual – Small Business Edition

For installation a bash compatible shell and bzip2 is required.

The minimum hardware requirements are:

- Intel Pentium III 1 GHz or compatible
- 256 MB RAM
- ~ 200 MB of hard disk space

## Appendix A – Settings Descriptions

Setting	Description
ApplicationLauncher.xservercheck.iorTimeout	Specifies the CORBA timeout for checking the xserver
ApplicationLauncher.xservercheck.retries	Specifies the number of xserver checks done
ApplicationLauncher.xservercheck.sleep	Specifies the time in milli seconds [ms] between the checks if the xserver has been started properly
Applications.authclient.command	Specifies the command to the authentication client binary
Applications.authclient.env	A list of environment variables used for starting the authentication client
Applications.authclient.parameters	The parameters passed to the authentication client binary
Applications.authclient.workingdir	Specifies the working directory for starting the authenticationclient
Applications.locale.command	Specifies the command for setting the locale. This can be any program which accepts a locale specification in the form of e.g. en, de, de_DE
Applications.locale.env	A list of environment variables used for starting the locale application
Applications.locale.parameters	Additional parameters to pass to the locale application
Applications.locale.workingdir	Specifies the working directory for starting the locale application
Applications.session.command	Specifies the command to the session application binary (e.g. kde, gnome, icewm,...). <b>Important:</b> see the Applications.session.env configuration setting to make sure the enviroment matches your executables.
Applications.session.env	A list of environment variables used for starting the session application. When using your own window managers please make sure to use your system environment settings. <b>Example values for custom applications:</b> PATH=\${PATH:+\$PATH:}/opt/thinstuff/rdpserver/bin LD_LIBRARY_PATH=\${LD_LIBRARY_PATH:+\$LD_LIBRARY_PATH:}/opt/thinstuff/rdpserver/lib The default setting might only work properly for applications provided in the application package (e.g. the default window manager).
Applications.session.parameters	The parameters passed to the session application
Applications.session.workingdir	Specifies the working directory for starting the session application
Applications.xserver.command	Specifies the command to the xserver binary
Applications.xserver.env	A list of environment variables used for starting the xserver
Applications.xserver.parameters	The parameters passed to the xserver executable (e.g. font paths, special backgrounds,...)
Applications.xserver.user	The user to run the started xservers as
Applications.xserver.workingdir	Specifies the working directory for started xservers
Match.groups.enable	This setting controls if this profile is matched by comparing group names
Match.groups.values	A list of groups who are used to select this profile
Match.hosts.enable	This setting controls if this profile is matched by comparing client hostnames

## Thinstuff Touch RDP Server – User Manual – Small Business Edition

Match.hosts.values	A list of client hostnames which are used to select this profile
Match.users.enable	This setting controls if this profile is matched by comparing user names
Match.users.values	A list of users who are used to select this profile
Network.ConnectionForwarding.socketrange.max	This is the end of the socketrange where the tcpforwarder will allocate ports for tcp forwarding to the X servers
Network.ConnectionForwarding.socketrange.min	This is the start of the socketrange where the tcpforwarder will allocate ports for tcp forwarding to the X servers
Network.ConnectionForwarding.timeout.sec	<b>INTERNAL:</b> this is the tcp forwarder thread socket finished/error/exception checking interval (the seconds part)
Network.ConnectionForwarding.timeout.usec	<b>INTERNAL:</b> this is the tcp forwarder thread socket finished/error/exception checking interval (the microseconds part)
Network.RDP.port	The port to listen on for incoming RDP client connections
RdpServer.alwaysSendTrueCursorKeys	<p>Some applications (most notably Oracle Forms) seem to have problems with keypad cursor keys. They do not react to xmodmap redefinition of those keys (probably use actual scancode) and some clients (e.g: Windows CE 5.0 on Symbol PDA) send cursor keys as keybad cursor keys. By setting this value to true, the rdp server redefines scancodes for these keys to always behave like actual cursor keys. Use with caution, and don't tamper with it if your setup is working as intended as it might destroy normal operation of the numpad area.</p> <p><b>Possible Values:</b> [false, true]  <b>Recommended Value:</b> false  <b>Default Value:</b> false</p>
RdpServer.BitmapCache.cacheHistorySize	<p>The cache history size determines how many tiles the server keeps in memory, to determine usage frequency. A bigger history size will result in tiles being kept longer in cache before being evicted by newer tiles. Smaller sizes will allow the cache to evict tiles faster, resulting in better performance when the cached tiles become obsolete often and quickly (eg: during browsing). This also affects memory performance, and is affected by the tileSize below. Bigger tileSize need smaller caches to be effective.</p> <p><b>Possible Values:</b> [1 .. 2^32-1]  <b>Recommended Values:</b> [1024 .. 16384]  <b>Default Value:</b> 16384</p>
RdpServer.BitmapCache.limitCacheSize	<p>limitCacheSize can be used to artificially limit the cache size used on the client. Usually it is not a good idea to use this, unless certain clients refuse to work, or memory limits on the client are extremely tight.</p> <p><b>Possible Values:</b> [0 (off), 1 .. 2^32-1]  <b>Recommended Value:</b> 0  <b>Default Value:</b> 0</p>
RdpServer.BitmapCompressor.enableRLECompression	Allow RLE compression to be used for bitmap data. RLE Compression is performed before and independently of RDP compression. Usually there is no reason to turn this off, but in certain environments where bandwidth does not matter (e.g: LANs) not using compression might improve CPU usage and latency. Note however that because of the

## Thinstuff Touch RDP Server – User Manual – Small Business Edition

	<p>increased strain on the RDP compressor, encryption and/or the network itself, the opposite may be true, your mileage may vary.</p> <p><b>Possible Values:</b> [false, true]  <b>Recommended Value:</b> true  <b>Default Value:</b> true</p>
RdpServer.BitmapRequest.cacheLimit1	<p>Updates smaller than this in a single direction will always be sent uncached, since sending a full tile for them is unlikely to bring any gain.</p> <p><b>Possible Values:</b> [0 (off), 1.. 2^32-1]  <b>Recommended Values:</b> [1 .. tileSize/4]  <b>Default Value:</b> 4</p>
RdpServer.BitmapRequest.cacheLimit2	<p>Updates with fewer pixels than this in total will always be sent uncached, since sending a full tile for them is unlikely to bring any gain.</p> <p><b>Possible Values:</b> [0 (off), 1.. 2^32-1]  <b>Recommended Values:</b> [1 .. tileSize*tileSize/16]  <b>Default Value:</b> 256</p>
RdpServer.BitmapRequest.sendBoundsFactor	<p>Complex regions are sent as a series of update rectangles if the sum of areas of the rectangles, compared to the area of the bounding rectangle is lower than this factor, otherwise it is sent by sending the bounding rectangle.</p> <p><b>Possible Values:</b> [0 .. 1]  <b>Recommended Values:</b> [0.7 .. 0.9]  <b>Default Value:</b> 0.8</p>
RdpServer.Connection.desiredFlushSize	<p>Preferred packet size. Smaller packets result in faster responses from the server at the expense of bandwidth efficiency. Especially on very slow connections (isdn) lower values may greatly increase the perceived performance for interactive work (office, ...).</p> <p><b>Possible Values:</b> [0 .. 16384]  <b>Recommended Values:</b> [1024 .. 8192]  <b>Default Value:</b> 8192</p>
RdpServer.Connection.enableFastCompression	<p>Enabling this flag results in a slightly different hash algorithm to be used in the rdp compressor. This results in about 5-10% worse compression quality, but improves compression speed by 5-10%.</p> <p><b>Possible Values:</b> [false, true]  <b>Recommended Value:</b> false  <b>Default Value:</b> false</p>
RdpServer.Connection.enableRdp2Compression	<p>Allow the improved compression of newer rdp clients to be used. Usually you always want this on since the newer compression gives better performance and better compression quality (up to 30%).</p> <p>Turn this off, if the client erroneously reports support for the new compression although it is not present (currently no such client is known). Ignored if enableRdpCompression is false. Note that even if set to true, the server will not use compression if it is not supported by the client, so it is safe to leave this on true.</p> <p><b>Possible Values:</b> [false, true, not-set (client controlled)]  <b>Recommended Value:</b> true  <b>Default Value:</b> not-set (client controlled)</p>
RdpServer.Connection.enableRdpCompression	<p>Allow compression to be used. Compression gives a big improvement in bandwidth and you usually want compression on. In certain environments where bandwidth does not matter (e.g: LANs) not using compression might</p>

## Thinstuff Touch RDP Server – User Manual – Small Business Edition

	<p>improve CPU usage and latency. Note however that because of the increased strain on the RDP compressor, encryption and/or the network itself, the opposite may be true, your mileage may vary. Note that even if set to true, the server will not use compression if it is not supported by the client, so it is safe to leave this on true.</p> <p><b>Possible Values:</b> [false, true, not-set (client controlled)]  <b>Recommended Value:</b> true  <b>Default Value:</b> not-set (client controlled)</p>
RdpServer.defaultBellFrequency	Default Settings for the system beep frequency. If no other parameters are set by a program, then this values will be used
RdpServer.defaultBellTime	Settings for the system beep bell time. If no other parameters are set by a program, then this values will be used
RdpServer.enableBitmapCache	Allow the usage of the bitmap cache. Usually you always want to enable this, since it provides great increases in performance. Disable this if the cache is not working correctly, or if you have special needs (e.g: multimedia applications in a LAN environment) <b>NOTE:</b> this also disables any usage of the ImageBuffer
RdpServer.ImageBuffer.allowSplitting	<p>Allow splitting of tiles. This allows splitting of tiles along a horizontal axis when updates do not need a full tile to be sent. Tiles are re-merged later automatically. This can improve bandwidth by sending less image data, but more tiles are generated which leads to worse cache usage. Overall the gain is usually higher for typical desktop work when turning this on.</p> <p>Scrolling and internet browsing might benefit from this setting.</p> <p><b>Possible values:</b> [false, true]  <b>Recommended value:</b> true  <b>Default value:</b> true</p>
RdpServer.ImageBuffer.hashMultiplier	<p>Hash base and multipliers. Subhashes are calculated as <math>((base + array[0])*multiplier + array[1])*multiplier \dots</math>. Hashes are calculated as <math>(subhash[0]*multiplier+subhash[1])*multiplier \dots</math>. Multipliers should result in good distribution of bits (e.g: prime numbers)</p> <p><b>Possible values:</b> [1 .. <math>2^{32-1}</math>]  <b>Recommended values:</b> any prime number  <b>Default Values:</b> 31 (multiplier), 2166136261 (base)</p>
RdpServer.ImageBuffer.subHashBase	The subhash base for hash calculation (see hashMultiplier for more details)
RdpServer.ImageBuffer.subHashMultiplier	The subhash multiplier for hash calculation (see hashMultiplier for more details)
RdpServer.ImageBuffer.tileSizeX	<p>Initial X tile size. X size is fixed, Y size can vary from [1 .. tileSizeY]. Smaller tile sizes usually result in faster transmission, while large sizes result in a bigger cache usage.</p> <p><b>Possible values:</b> [1 .. 64]  <b>Recommended values:</b> [32, 48, 64]  <b>Default values:</b> 64x64</p>
RdpServer.ImageBuffer.tileSizeY	<p>Initial Y tile size. X size is fixed, Y size can vary from [1 .. tileSizeY]. Smaller tile sizes usually result in faster transmission, while large sizes result in a bigger cache usage.</p>

## Thinstuff Touch RDP Server – User Manual – Small Business Edition

	<b>Possible values:</b> [1 .. 64] <b>Recommended values:</b> [32, 48, 64] <b>Default values:</b> 64x64
RdpServer.LinesRequest.extendLines	<p>The RDP protocol does not draw the endpoints of a line, while the X server does. This leads to minor graphical inconsistencies. Order translation tries to alleviate this by extending lines for one pixel so that the resulting RDP operation should exhibit the same behaviour as the original X request.</p> <p>However, rdesktop clients up to version 1.4.1 do ignore this minor detail and produce lines which include the last point, staying true to the original X method of drawing things. In this case the above mentioned fix causes lines to overshoot by one pixel. rdesktop clients should be autodetected, but if this does not work correctly you can try to change this setting to manually disable the line extension.</p> <p><b>Possible Values:</b> [false, true]  <b>Recommended Value:</b> true  <b>Default Value:</b> true</p>
RdpServer.MTU	<p>The maximum transferable unit within the RDP protocol translation. Adjust this setting to match your transport layer (e.g. ethernet, internet routing,...)</p>
RdpServer.ProtocolTracer.fontAliasThreshold	<p>Allow antialiased fonts to be sent as aliased fonts. RDP has no notion of antialiased fonts, therefore antialiased text must be sent as bitmaps if pixel perfect representation is desired.</p> <p>It is however possible to convert antialiased fonts back to aliased fonts, resulting in less bandwidth usage at the expense of image quality. The following setting controls how and if fonts are converted. Note that higher numbers will result in fonts to appear lighter, while lower ones make them appear bolder.</p> <p><b>Possible Values:</b> [0 (off), 1 .. 255]  <b>Recommended Values:</b> [0 (off), 112 .. 140]  <b>Default Value:</b> 0</p>
RdpServer.Translator.queueSize	<p>The maximum number of requests (pseudo rdp operations) to be queued between the protocol tracer and the actual translator. Lower values will make the Xserver block faster if the network connection is slow (or start spoiling more aggressively), while higher values give the server more time to ease out short bottlenecks in bandwidth. Lower values will produce tighter realtime behavior at the expense of bandwidth and/or update frequency, while higher values will result in a general smoother experience at the expense of RAM and responsiveness.</p> <p><b>Possible Values:</b> [2 .. 2^32-1] <b>NOTE:</b> do not set to 0 or 1 !  <b>Recommended Values:</b> [2 (synchronized mode), 64 (multimedia) .. 1024 (office) ]  <b>Default Value:</b> 64</p>
RdpServer.UseWebServer	<p>Enable this setting to enable the internal debug webserver of each xserver</p>
RdpServer.verifyDisconnect	<p>Bring up the "Do you really want to disconnect?" dialog when pressing the X button.</p> <p><b>Possible values:</b> [false, true]  <b>Recommended value:</b> true</p>

## Thinstuff Touch RDP Server – User Manual – Small Business Edition

	<b>Default value:</b> true
RdpServer.WebPortBase	This setting specifies the webserver portbase for the xserver internal debugging webserver. Webservers try to find an available port by starting at this value
Security.Authentication.alwaysShowChooser	This setting may enable the session chooser to be always displayed and not only for handling the special cases where a single user has multiple sessions. This makes it possible to create further parallel sessions for one user
Security.Authentication.authenticationProfile	The configuration profile to use during the logon process
Security.Authentication.authenticationUsername	The system username to use for starting applications for the logon process
Security.Authentication.performEarlyAuthentication	Specifies if the terminal server should check the username and password directly provided by the clients (and thus maybe allow them to logon without ever having to enter a password in the logon dialog)
Security.Authentication.performLateAuthentication	Specifies if the terminal server should show a logon dialog if early authentication (sending username and password with the client) either failed or was disabled. If this is false and early authentication fails the connection will be closed
Security.RDP.CACert	The certification authority certificate (CA cert) to use for the encryption process
Security.RDP.ClientCert	The client certificate to use for RDP encryption. This cert is sent to all clients
Security.RDP.CryptoVersion	RDP cryptography version, the only valid value is 5
Security.RDP.KeyLength	The key length for the symmetric encryption in bytes. The only valid value is 16
Security.RDP.ProtocolVersion	RDP protocol version, the only valid value is 5
Security.RDP.ServerCert	The server certificate to use for RDP encryption
Security.RDP.ServerKey	The server private key to use for RDP encryption
Session.DisplayAllocation.max	Specify the upper limit for the range of display numbers to use for sessions in this profile. <b>Possible values:</b> [0 .. 65535] <b>Recommended value:</b> at least 100 higher than min <b>Default value:</b> 65536
Session.DisplayAllocation.min	Specify the lower limit for the range of display numbers to use for sessions in this profile. <b>Possible values:</b> [0 .. 65535] <b>Recommended value:</b> at least 100 lower than max <b>Default value:</b> 100
Session.matchPerClientHost	Enable this setting if existing sessions should be reconnected by matching the client hostname
Session.matchPerUser	Enable this setting if existing sessions should be reconnected by matching the username
Session.maxDepth	Specify the maximum color depth a client can use. Warning: 24 bit color depth may result in higher CPU usage if clients do not actually connect in 24bit mode. It is recommended that 16bit mode is used unless 24bit mode is explicitly needed. <b>Possible values:</b> 8, 16, 24 <b>Recommended values:</b> 16 <b>Default value:</b> 16
Session.maxHeight	Specify the maximum height of the resolution a client can use. Note that very high values will result in high memory

## Thinstuff Touch RDP Server – User Manual – Small Business Edition

	usage of sessions, even if the client is connected with a much lower resolution. <b>Possible values:</b> [1 .. 65535] <b>Recommended values:</b> 480, 600, 768, 1024, 1200, 1536 <b>Default value:</b> 1200
Session.maxWidth	Specify the maximum width of the resolution a client can use. Note that very high values will result in high memory usage of sessions, even if the client is connected with a much lower resolution. <b>Possible values:</b> [1 .. 65535] <b>Recommended values:</b> 640, 800, 1024, 1280, 1600, 2048 <b>Default value:</b> 1600
Session.startApplication	Enable this setting to start the session application for all sessions started with this profile
Session.timeout	The timeout in seconds until a running session without connected clients is kept alive before killing it (-1 means forever, 0 means that the session is killed after the last client disconnects)